

Acceptable Use Policy

The rules for responsible use of company and client systems, data, and devices.

Version: 1.0 · **Last updated:** December 2025 · **Owner:** Security Lead

1. Purpose

To define acceptable use of Backpack Works information systems, devices, accounts, and data.

2. Scope

All personnel who use company systems or access client data.

3. Acceptable use

- Use company systems and client data only for legitimate business purposes.
- Protect credentials; never share passwords and always use MFA where available.
- Store company and client data only in approved systems.
- Access client source code repositories and production databases (e.g. Supabase) only from a company work laptop. Mobile device use is limited to email and Slack.
- Lock devices when unattended and report lost or stolen devices immediately.

4. Prohibited use

- Sharing confidential or client data with unauthorized parties.
- Installing unapproved or pirated software.
- Disabling security controls (encryption, anti-malware, screen lock).
- Using personal accounts or unapproved tools to process client data.
- Accessing client source code repositories or production databases from mobile or personal devices.
- Entering confidential client data or secrets into public AI tools that may use it for training.

5. Monitoring

Company systems may be monitored for security and compliance purposes, consistent with applicable law.

6. Enforcement & review

Violations may result in disciplinary action. This policy is reviewed at least annually.